CLAIMS

1. A security communication packet processing apparatus that performs at least one of encryption processing, decryption processing and authentication processing to a packet comprising:

one or more encryption processing unit operable to perform the encryption processing and the decryption processing in a data block unit of B1 bits;

one or more authentication processing unit operable to perform the authentication processing in a data block unit of B2 (= n x B1) bits in parallel to the encryption processing or the decryption processing by the encryption processing unit, and output an authentication value indicating the result of the authentication processing;

one or more data block accumulation unit operable to accumulate the data blocks to which the encryption processing is performed by the encryption processing unit, and, when the accumulated amount of the data blocks reaches B2 bits, output the data blocks to the authentication processing unit;

a packet construction unit operable to receive the encrypted or decrypted data blocks from the encryption processing unit, receive the authentication value from the authentication processing unit, and construct a packet including the received data blocks and authentication value; and

a control unit operable to divide the inputted packet into the data blocks of B1 bits, and output the data blocks sequentially to the encryption processing unit.

2. The security communication packet processing apparatus according to Claim 1,

wherein the control unit judges which type the inputted

packet is, the first type packet requiring the encryption processing and the authentication processing, the second type packet requiring the decryption processing and the authentication processing, the third type packet requiring one of the encryption processing and the decryption processing, or the fourth type packet requiring the authentication processing only,

when the packet is judged to be the first type packet, divides the packet into the data blocks of B1 bits and outputs the data blocks sequentially to the encryption processing unit ,

when the packet is judged to be the second type packet, divides the packet into the data blocks of B1 bits, outputs them sequentially to the encryption processing unit, divides the packet or the duplicate of the packet into the data blocks of B2 bits, and outputs the data blocks sequentially to the authentication processing unit,

when the packet is judged to be the third type packet, divides the packet into the data blocks of B1 bits and outputs the data blocks sequentially to the encryption processing unit, and

when the packet is judged to be the fourth type packet, divides the packet into the data blocks of B2 bits and outputs the data blocks sequentially to the authentication processing unit.

3. The security communication packet processing unit according to Claim 1,

wherein the number of at least one of the encryption processing unit and the authentication processing unit is two or more, and

the number of the data block accumulation unit is equal to that of the encryption processing unit.

4. The security communication packet processing apparatus according to Claim 3,

wherein the control unit specifies, among two or more encryption processing units or two or more authentication processing units, the encryption processing unit or the authentication processing unit that is ready for processing, and outputs the data blocks to the specified encryption processing unit or the authentication processing unit.

5. The security communication packet processing apparatus according to Claim 1 further comprising:

a data path connection switching unit that can connect the output of the control unit and the input of the encryption processing unit, the output of the control unit and the input of the authentication processing unit, the output of the encryption processing unit and the input of the data block accumulation unit, and the output of the data block accumulation unit and the input of the authentication processing unit, respectively and independently.

6. The security communication packet processing apparatus according to Claim 5,

wherein the control unit judges which type the inputted packet is, the first type packet requiring the encryption processing and the authentication processing, the second type packet requiring the decryption processing and the authentication processing, the third type packet requiring one of the encryption processing and the decryption processing, or the fourth type packet requiring the authentication processing only,

when the packet is judged to be the first type packet,

controls the data path connection switching unit so as to connect the output of the control unit and the input of the encryption processing unit, the output of the encryption processing unit and the input of the data block accumulation unit, and the output of the data block accumulation unit and the input of the authentication unit,

when the packet is judged to be the second type packet, controls the data path connection switching unit so as to connect the output of the control unit and the input of the encryption processing unit, and the output of the control unit and the input of the authentication unit,

when the packet is judged to be the third type packet, controls the data path connection switching unit so as to connect the output of the control unit and the input of the encryption processing unit, and

when the packet is judged to be the fourth type packet, controls the data path connection switching unit so as to connect the output of the control unit and the input of the authentication processing unit.

7. The security communication packet processing apparatus according to Claim 6,

wherein the number of at least one of the encryption processing unit and the authentication processing unit is two or more, and

the number of the data block accumulation unit is equal to that of the encryption processing unit.

8. The security communication packet processing apparatus according to Claim 7,

wherein the control unit specifies, among two or more encryption processing units or two or more authentication

processing units, the encryption processing unit or the authentication processing unit that is ready for processing, and makes the data path connection switching unit perform a connection for the specified encryption processing unit or the authentication processing unit.

9. The security communication packet processing apparatus according to Claim 1 further comprising:

a processing data saving unit, for each of at least one of the encryption processing unit, the authentication processing unit and the data block accumulation unit, that has a memory area for temporarily saving the data blocks which are being processed in the processing unit corresponding respectively to the processing unit.

10. The security communication packet processing apparatus according to Claim 9,

wherein the control unit specifies the processing unit that is performing the processing of the data blocks of the packet with the lowest priority among the processing units, and after saving the data blocks which are being processed in the processing unit into the processing data saving unit, makes the processing unit perform the processing of the data blocks of the inputted packet.

11. The security communication packet processing apparatus according to Claim 10 further comprising:

the data path connection switching unit that can connect the output of the control unit and the input of the encryption processing unit, the output of the control unit and the input of the authentication processing unit, the output of the encryption processing unit and the input of the data block accumulation

unit, and the output of the data block accumulation unit and the input of the authentication processing unit, respectively and independently.

12. The security communication packet processing apparatus according to Claim 11,

wherein the number of at least one of the encryption processing unit and the authentication processing unit is two or more, and

the number of the data block accumulation unit is equal to that of the encryption processing unit.

13. The security communication packet processing apparatus according to Claim 1 further comprising:

the processing data saving unit, for each of at least two of the encryption processing unit, the authentication processing unit and the data block accumulation unit, that has a memory area shared by the processing units for temporarily saving the data blocks which are being processed in the processing units.

14. The security communication packet processing apparatus according to Claim 13,

wherein the control unit specifies, among the processing units, the processing unit that is performing the processing of the data blocks of the packet with the lowest priority, and after saving the data blocks which are being processed in the processing unit in the processing data saving unit, makes the processing unit perform the processing of the data blocks of the inputted packet.

15. The security communication packet processing apparatus according to Claim 14 further comprising:

the data path connection switching unit that can connect the output of the control unit and the input of the encryption processing unit, the output of the control unit and the input of the authentication processing unit, the output of the encryption processing unit and the input of the data block accumulation unit, and the output of the data block accumulation unit and the input of the authentication processing unit, respectively and independently.

16. The security communication packet processing apparatus according to Claim 15,

wherein the number of at least one of the encryption processing unit and the authentication processing unit is two or more, and

the number of the data block accumulation unit is equal to that of the encryption processing unit.

17. The security communication packet processing apparatus according to Claim 1,

wherein the B1 is 64, and

the B2 is 512.

18. A security communication packet processing method that performs at least one of the encryption processing, decryption processing and the authentication processing to the packet including:

a dividing step for dividing the inputted packet into the data blocks of B1 bits;

an encryption processing step for performing the encryption processing or the decryption processing to the divided data blocks of B1 bits;

a data block accumulating step for accumulating the

encrypted data blocks and outputting the data blocks when the accumulated amount of the data blocks reaches B2 (= n x B1) bits;

an authentication processing step for performing the authentication processing to the outputted data blocks of B2 bits in parallel to the encryption processing or the decryption processing, and outputting the authentication value indicating the result of the authentication processing;

a packet constructing step for receiving the encrypted or decrypted data blocks, receiving the authentication value, and constructing the packet including the received data blocks and authentication value.

19. The security communication packet processing method according to Claim 18 further including:

a control step for judging which type the inputted packet is, the first type packet requiring the encryption processing and the authentication processing, the second type packet requiring the decryption processing and the authentication processing, the third type packet requiring only one of the encryption processing and the decryption processing, or the fourth type packet requiring the authentication processing only, and when it is judged to be the first type packet, controlling so that the division in the dividing step, the encryption processing in the encryption processing step, the accumulation in the data block accumulating step, the authentication processing in the authentication processing step and the construction in the packet constructing step are performed.